Secure Technology Environment and Best Practices

MINIMUM BASELINE OF CYBERSECURITY

Goal 4: Secure Technology Environment and Best Practices

Minimum Baseline of IT

The purpose of this document is to guide municipalities in the creation of an effective cybersecurity program and to standardize on a foundational level of information technology (IT) policies and practices in their environment. The Minimum Baseline of IT, as part of **Goal 4 of the Minimum Baseline of Cybersecurity**, is a set of recommendations for municipalities to meet this foundational level of IT. The definition "municipality" encompasses communities, generally made up of citizens, local government, schools, public safety, and utilities.

The Minimum Baseline of IT outlines these policies and practices and describes the core components of day-to-day IT operations that are required to establish a robust cybersecurity program. This is the fundamental information municipal executives need to know to communicate with their IT department or Managed Service Provider (MSP) or other contracted services. Robust IT services, as provided by internal IT and/or an MSP, are necessary to support the business objectives of the organization.

- Identify and engage with municipal business process owners
  - Understand business process to evaluate risks, recovery time objective (RTO) and recovery point objective (RPO)
  - Identify, classify, and protect data in accordance with regulations set forth by standards such as **Criminal Justice Information Services (CJIS)**, **Health Insurance Portability and Accountability Act (HIPAA)**, or data containing **personally identifiable information (PII)**
  - Conduct a **"crown jewel" analysis** – identify your most critical data and systems
  - Establish a working group for the purpose of **developing a cyber incident response plan (IRP)** for your organization. Your IRP should include IT policies and procedures.
  - An IRP communications policy should be created for notifying partner networks of incidents, such as state systems (CJIS, Secretary of the Commonwealth's Office) and any other systems specific to your organization (third-party vendors or applications).

- Maintain an accurate asset inventory that includes equipment and software
  - Deploy a remote monitoring and management (RMM) Tool to perform patching and inventory management. Your MSP should provide an RMM tool that patches operating systems and third party software.
  - Keep software, network, and server equipment up to date with the latest patches or versions
  - Plan for legacy systems that cannot be updated: identify risks and implement programs to mitigate risks
  - Implement email SPAM filter
  - Implement endpoint detection and response (EDR)
  - Reassess inventory at least annually
  - Plan for a five-year refresh cycle on IT equipment

- Consider the physical security and environmentals of your systems as an important aspect of your cybersecurity and resiliency posture.

- Use business class IT services and equipment (vs. consumer class)
  - Engage your internal IT or hire a reliable MSP for proactive support
    - Reference **ITS74ProjServ & ITS78 Statewide Contract for Data, Cybersecurity, and Related Audit, Compliance, and Incident Responses Services** contracts to find an MSP

- Engage with cloud service providers that are government compliant and use products and services that are government certified (ie. Microsoft Government Community Cloud (GCC) vs. Microsoft Commercial Cloud)
- Consider virtual Chief Information Officer (CIO) services with your MSP for the development of your strategy
- Implement network segmentation, access control lists (ACLs), advanced logging/monitoring
- Follow the National Institute of **Standards and Technology (NIST) SP 800-171** or **Center for Internet Security (CIS) 18** security frameworks
- Install a next generation firewall (NGFW), which includes:
  - Anti-malware
  - Anti-virus
  - Content filtering
  - Botnet protection
- Domain Name System (DNS) protection – MS-ISAC offers a **free malicious domain blocking and reporting service** to municipalities
- If Security Operations Center (SOC) not included with MSP services, then engage SOC provider to obtain:
  - Logging and traffic analysis
  - Threat hunting
  - Identification of indicators of compromise (IoCs) and response

- Maintain active support agreements with vendors and confirm they have disaster recovery services for both cloud and in-house products/services for ALL municipal software platforms

- Create a password policy that requires strong passwords or pass-phrases
  - Use your directory service (e.g. Active Directory) to enforce

- Enforce **Multi-factor Authentication (MFA)**
  - At a minimum, on VPN and email

- Implement a Backup Strategy
  - Implement the **3-2-1 standard** – 3 copies of the backup, 2 types of media, 1 offsite
  - Become **Immutable** – to reduce ransomware impact
  - Follow federal, **state**, and local laws for records retention.
  - Be sure to **test** your ability to restore from backups regularly

- Conduct annual **Vulnerability Scanning –** a verification of your system security. (CISA offers a free vulnerability scan. For more information go to: **https://www.cisa.gov/cyber-hygiene-services**; Executive Office of Technology Services and Security Office of Municipal and School Technology also offers free **Health Checks**)

- Annual Cybersecurity Awareness Training, at a minimum for all users with access to municipal IT systems. (The Executive Office of Technology Services and Security Office of Municipal and School Technology offers a **free municipal cybersecurity awareness training grant program**)